AU/AWC/RWP059/1998-04

AIR WAR COLLEGE

AIR UNIVERSITY

GLOBAL ENGAGEMENT: BUILDING CASTLES ON SAND?

by

Carla D. Bass, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Dr. George J. Stein

Maxwell Air Force Base, Alabama

April 1998

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (FROM - TO)
01-04-1998	Thesis	xx-xx-1998 to xx-xx-1998

4. TITLE AND SUBTITLE
Global Engagement: Building Castles on Sand?
Unclassified

5a. CONTRACT NUMBER
5b. GRANT NUMBER
5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Bass, Carla D. ;

5d. PROJECT NUMBER
5e. TASK NUMBER
5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME AND ADDRESS
Air War College
Maxwell AFB, AL36112

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS
,

10. SPONSOR/MONITOR'S ACRONYM(S)
11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APUBLIC RELEASE
,

13. SUPPLEMENTARY NOTES

14. ABSTRACT
Good news...US national-level policy and military doctrine, at Joint and Service levels, now recognize Information as a specific domain in which to conduct operations, paralleling that of air, land, and sea. They realize wars can be fought and lost in the information domain. Conducting information operations without effective opposition, defined as ?Information Superiority?, can be as crucial as air superiority to the outcome of war. Information Superiority now stands as one of six Joint operational concepts and as one of six Air Force core competencies. AFDD 1-1 states, ?Dominating the information spectrum is as critical to conflict now as controlling air and space, or as occupying land was in the past, and is seen as an indispensable and synergistic component of air and space power.?3 This concept expands the battle domain formerly recognized only as air, land, and sea.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	Public Release	70	Fenster, Lynn lfenster@dtic.mil
Unclassified	Unclassified	Unclassified			19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number 703767-9007 DSN 427-9007

Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Page

Illustrations

Page

Tables

Page

Acknowledgements

I wish to thank several individuals for their insights and sage advise as I wrote this paper. Many of these professionals are located at Headquarters, Air Intelligence Agency, an organization recognized by senior Air Force leaders for innovative and leading-edge contributions to IO concepts and application. Particularly generous with their time were: Brigadier General Rider, AIA/CV; Colonel Gary Harvey, 67 IW/CC; Colonel Alan Thomas, Special Assistant to AIA/CC; and Mr. Lynn Reeves of AIA's Information Operations Center. Joint Command and Control Warfare Center (JC2WC) was especially helpful. Here, I wish to thank Colonel Frank Goral, JC2WC/CV. Colonel Richard Szafranski, USAF (Ret), certainly helped give the paper added depth, especially regarding potential alternatives for a DOD organization to better face challenges posed in the Information Age. Finally, I wish to thank my advisor, Dr. George J. Stein for both his IO class and suggestions on this paper. Of course, any shortfalls contained herein are exclusively my own.

Abstract

> The United States can not simply postulate doctrine and tactics which rely so extensively on information and information technology without comparable attention to information and information systems protection and assurance. This attention, backed up with sufficient resources, is the only way the Department can ensure adequate protection of our forces in the face of the inevitable information war.
>
> Defense Science Board[1]

> Dominating the information spectrum is as critical to conflict now as controlling air and space, or as occupying land was in the past....Whoever has the ability to gain, defend, exploit, and attack information, and deny the same capabilities to an opponent, has a distinct strategic advantage.
>
> AFDD 1-1[2]

Good news...US national-level policy and military doctrine, at Joint and Service levels, now recognize Information as a specific domain in which to conduct operations, paralleling that of air, land, and sea. They realize wars can be fought and lost in the information domain. Conducting information operations without effective opposition, defined as "Information Superiority", can be as crucial as air superiority to the outcome of war. Information Superiority now stands as one of six Joint operational concepts and as one of six Air Force core competencies. AFDD 1-1 states, "Dominating the information spectrum is as critical to conflict now as controlling air and space, or as occupying land was in the past, and is seen as an indispensable and synergistic component of air and space power."[3] This concept expands the battle domain formerly recognized only as air, land, and sea.

Bad news...policy, doctrine, and planning documents such as Joint Vision 2010 and USAF Global Engagement assume the US will have unimpeded access to information on our own forces, and on the enemy as well, due largely to our technological sophistication. They propose application of a downsized US military in a still very deadly world...based on the premise of Information Superiority.

> Information operations conducted by air and space forces enable the Joint Force Commander (JFC) to have dominant battlespace awareness in order to economically allocate forces for maximum effect.
>
> AFDD 1-1[4]

However, the cautious reader might ask whether the US military has based its policy not on a firm foundation, but rather has built castles on sand. Indeed, the Defense Science Board cited this point most eloquently in its report delivered to the Secretary of Defense in November, 1996.

> [Services] can not simply postulate doctrine and tactics which rely so extensively on information systems protection and assurance. This attention, backed up with sufficient resources, is the only way the department can ensure adequate protection of our forces in the face of the inevitable information war.[5]

A missing ingredient to our firm foundation is Information Assurance…the certain readiness, reliability, integrity, and continuity of our communication systems, intelligence systems, data bases, and supporting civilian infrastructure. All are necessary to successfully conduct military operations. The US will not achieve Information Superiority until we first secure our own information systems and convince adversaries that our systems are resilient. This involves calculated risk management: identifying, protecting, making robust, and reconstituting those processes most critical to national

defense, similar to Continuity of Government operations undertaken during the Cold War. Furthermore, we must expand our own offensive capabilities by developing Information Warfare techniques and clearly convey to adversaries that extant capability and our willingness to apply it, when necessary. This is the principle of deterrence applied to what is now known as Information Operations or the "fifth battlespace domain."

Organizations throughout DOD now focus effort, energy, and funding towards protecting military components of the information infrastructure. The USAF has been particularly active with initiatives such as creation of the Air Force Information Warfare Center (AFIWC) and recent establishment of the Information Warfare Battlelab. Air Intelligence Agency's (AIA) CYBERWATCH is another critical first step towards attaining Information Assurance which focuses on the ability to detect, identify, and react to an electronic intruder. This field is new, capabilities are still evolving (both friendly and adversary), and numerous issues must yet be resolved. One large question looms, that of organization. Who is in charge? Which organization should orchestrate the many, diverse attempts to secure military information systems? Does the DOD need a Commander in Chief (CINC) for Information Operations. If so, whom?

This paper will attempt to prove that a CINC for IO is now necessary to capture the plethora of ongoing IO-related activities and hone them into a single, powerful, coordinated capability. Furthermore, using Special Operations Command (SOCOM) as a model, Information Operations Command or an extant Unified Command should be allocated a designated program element to eliminate sporadic, uncoordinated, and

oftentimes insufficient IO expenditures and to more efficiently distribute lessons-learned across the DOD.

Notes

[1] Defense Science Board, Task Force on Information Warfare-Defense (IW-D), November 1996, Section 2.1.

[2] Air Force Doctrine Document (AFDD) 1-1, *Air Force Basic Doctrine*, September 1997, pg 32.

[3] Ibid., pg 31.

[4] Ibid., pg 18.

[5] Defense Science Board, *Task Force on Information Warfare-Defense (IW-D),* November 1996, Section 2.1.

Chapter 1

In The Beginning, There Was IO

> *In preparations for national defense we have to follow an entirely new course because the character of future wars is going to be entirely different from the character of past wars...we had better get accustomed to this idea and prepare ourselves for the new conflicts to come.*
>
> —Douhet[1]

What exactly is Information Operations (IO)? DOD Directive S3600.1 and AFDD 1-1 both define IO as "actions taken to affect adversary information and information systems while defending one's own information and information systems."[2] Specifically, IO consists of operations security (OPSEC), psychological operations (PSYOP), deception, electronic warfare (EW), physical destruction, and especially from the USAF perspective, information attack. The concept of "attack" in an IO context spans the extreme from physical destruction, to impeding data flows, to covertly manipulating data content. The goal of IO is to obtain Information Superiority by employing some or all of these tools in a given strategy. AFDD 1-1 defines Information Superiority as, "the ability to collect, control, exploit, and defend information while denying an adversary the ability to do the same and, like air and space superiority, includes gaining control over the information realm and fully exploiting military information functions."[3] IO tools may be employed in support of air, land, sea, or space-based operations, or may be compiled into an IO campaign plan supporting strategic objectives. The military conducts IO

throughout the conflict spectrum, during all phases of an operation, and across the range of military operations. Information Warfare (IW) is the application of IO tools during a crisis or war.

The problem, however, is that many within the military do not, as yet, understand or support the validity of IO. Too often, IO is mistakenly and exclusively associated with offensive and defensive actions taken against automated information…i.e., computer warfare. This is a serious misunderstanding which undermines our ability to protect the US from IO attacks and impedes development of successful counter and offensive IO strategies. IO is conducted daily, although not always recognized as such. For example, diplomats employ IO as demonstrated by recent verbal sparring between Iraq and the US. As seen here, psychological aspects of IO sometimes approximate the game of poker, employing techniques of bluffing while trying to ascertain strengths of the opponent's hand. If not carefully considered, IO strategies can backfire as seen in the town meeting held in February 1998 at Ohio State University with Secretary of Defense Cohen, Secretary of State Madeline Albright, and National Security Advisor Sandy Berger. Rather than muster public support for an air strike against Iraq, the meeting highlighted to the world a lack of US concurrence on that very point. It is imperative for our national security that individuals, from national-level policy makers to editors of the evening news, understand the facets of IO and their own respective roles therein.

The concept of IO provokes strong reactions. The first is frustrated confusion due to the plethora of newly developed, service-specific, and frequently changing IO terminology, as illustrated by the figure below.[4]

Figure 1. IO Terms

Skeptics eagerly point out what they call, "terminology creep," noting the gradual escalation of phrases such as "password security", "computer security", "information systems security", "information protection", and the latest, "information warfare." They suggest, somewhat correctly, that project managers often claim IO associations to gain easier access to funding.[5] So much energy is wasted grappling with bureaucratic nuances, individuals essential to successfully conduct IO disengage out of impatience when faced with other completing operational priorities. This process damages the credibility of IO and even more importantly, wastes valuable time needed to develop and employ IO defensive measures.

Another reaction to IO parallels the response to air power in the first half of the 20th century. One extreme position staunchly advocates IO (some proponents are considered evangelists) while the other debunks the concept as little more than trendy terminology, elicited because funds are currently available for IO-affiliated projects. The pragmatic position lies somewhere in between. Why this intense response? Some early proponents of IO lost credibility, as did early advocates of air power, by claiming operational benefits far beyond that technically available. In the 1920's and into the early 1940's, visionaries of air power presaged capabilities that would not come to pass until much later in WWII. Billy Mitchell, for example, postulated that "nothing can stop the attack of aircraft except other aircraft." He predicted, "aerial torpedoes guided by gyroscopic instruments and wireless telegraphy." Regarding strategic bombing, he predicted that, "In the future, the mere threat of bombing a town by an air force will cause it to be evacuated and all work in factories to be stopped."[6] Strategists working in the Air War Plans Division-1 (AWPD-1) in August 1941 also overestimated capabilities of strategic air power. Thinking it unlikely that an Allied ground offensive could be executed in less than 3 years, AWPD-1 planners postulated that a successful air offensive campaign might negate the need for any ground forces. They thought air superiority would be won by bombers while pursuit aircraft would protect bases in a defensive role.[7] 8th Air Force subsequently sent large groups of unescorted heavy bombers deep into the German heartland. In contrast to expectations of early 1930's, this strategy was disastrous until technology caught up to strategy. Similarly, air power strategists in DESERT STORM oversold air power's potential with the plan INSTANT THUNDER, claiming that air power could win the war by executing 700 daily strikes deep in Iraq for six consecutive

days. The plan lost some credibility when it made no allowances to attack ground forces and could not respond to the question, "What happens after day six?"[8]

What were the over enthusiastic claims of IO? Enthusiasts championed IO as a truly unique form of warfare, otherwise known as a revolution in military affairs (RMA), a provocative statement in itself. They forecast dominant battlespace awareness, where wars would be fought and won exclusively in the electronic domain with virtual combat staffs zapping information across networks. Others make alarmist, Doomsday predictions of impending catastrophic attack on the US strategic information infrastructure, sometimes dramatically referred to as an "electronic Pearl Harbor."

Is IO a RMA or a just a logical extension of existing technology? Pragmatists argue the latter. Gain, exploit, defend, and attack. The fundamentals of information warfare--attacking an opponent's information while protecting and enhancing friendly information--have not changed through time. Information has been viewed as both target and weapon for thousands of years. Sun Tzu's principles, inculcated in disciples since 500 BC, liberally apply techniques such as spies, rumors, deception, and operational security. Sun Tzu regarded information as essential to war, "Delicate indeed! Truly delicate! There is no place where espionage is not used."[9] His philosophy was to wage a war of perceptions, manipulating data and public opinion; the target was the mind of his enemy. Military objectives included disrupting alliances; ascertaining enemy plans, strengths and weaknesses; and attacking enemy strategy. The ultimate objective for Sun Tzu's army was to subdue the enemy without fighting. He continues, "Those skilled in war subdue the enemy's army without battle. They capture his cities without assaulting them and overthrow his state without protracted operations."[10] Today, IO strategists apply Sun Tzu

principles powered by Information Age technology, supporting the argument that IO is not a RMA. Hopefully, this will remove some of the sensationalism decried by IO critics.

Pragmatists also downplay the impending onset of an "electronic Pearl Harbor." Such a coordinated strike across our infrastructure would require extensive, detailed intelligence on vulnerabilities spanning political, economic, and military systems. The President's Commission on Critical Infrastructure Protection (PCCIP) reached the same conclusion in its final report published in October 1997. "The Commission has not discovered an immediate threat sufficient to warrant a fear of imminent national crisis."[11] Another major study conducted by the Defense Science Board (DSB), "does not accept the assertions of popular press that a few individuals can easily bring the United States to its knees."[12] DSB assesses a major strategic disruption as "Low" by the year 2005.[13]

Threat Assessment	Validated Existence	Existence Likely but not Validated	Likely by 2005	Beyond 2005
Hacker	W	--	--	--
Disgruntled Employee	W	--	--	--
Crook	W	--	--	--
Organized Crime	L	--	--	--
Political Dissident	--	W	--	--
Terrorist Group	--	L	W	--
Foreign Espionage	L	--	W	--
Tactical Countermeasures	--	**W**	--	--
Orchestrated Tactical IW	--	--	**L**	**W**
Major Strategic Disruption of US	--	--	--	**L**

Table 1. Projected Threat Assesment

This discussion does not intimate, however, that IO can be ignored in the interim. Both studies assess the current IO threat as 'Significant' based on numerous intrusions,

system vulnerabilities, and an as yet minimal ability to detect, deter, and respond to these attacks. That same DSB report assesses as "Widespread" the threat of orchestrated tactical IW by the year 2005. While these two reports are significant, they are also dated. Technological developments spring forth almost overnight…so do capabilities of IO adversaries and subsequent vulnerabilities of the US infrastructure. Unfortunately, the structured, sophisticated computer attack waged against the DOD in February 1998 indicates the PCCIP and DSB threat assessments may now be overly optimistic.

Notes

[1] Douhet, *The New Form of War,* Air War College Strategy, Doctrine, and Airpower, Book II, Air University Press, August 1998, pg 28.

[2] Air Force Doctrine Document (AFDD) 1-1, *Air Force Basic Doctrine*, September 1997, pg 81.

[3] Ibid., pg 31.

[4] Figure 3-4-1 from "Information Warfare: Legal, Regulatory, etc.

[5] Michael A Dornheim, *Bombs Still Beat Bytes,* Aviation Week and Space Technology, January 19, 1998.

[6] Brig Gen William Mitchell, *The Development of Air Power*, Air War College Strategy, Doctrine, and Air Power Book II, Air University Press, August 1998, pg 32-37.

[7] Robert Frank Futrell, *AWPD-1:Air Planning for War*, Air War College Strategy, Doctrine, and Air Power Book II, Air University Press, August 1998, pg 93-97.

[8] Michael R. Gordon and Bernard E. Trainor, *Instant Thunder*, Air War College Strategy, Doctrine, and Air Power Book II, Air University Press, August 1998, pg 447-473.

[9] Sun Tzu, *The Art of War*, translated/edited by Samuel B. Griffith, Oxford University Press, 1971, pg 147.

[10] Ibid., pg 79.

[11] President's Commission on Critical Infrastructure Protection Final Report, pg x, October 1997, Robert T. Marsh, Chairman.

[12] Defense Science Board, *Task Force on Information Warfare-Defense*, November 1996, Duane P. Andrews, Chairman, Section 2.2.

[13] Ibid., Exhibit 2-6.

Chapter 2

A Whole New World

So, what is new? The most monumental change is the explosion of information technology and potential ramifications of a large-scale "malfunction." Military professionals agree that information technology affects the art of war. War has indeed evolved from applying information in war, also known as "intelligence", to focusing on information as a means to wage war, i.e., "Information Warfare." That importance has been reflected in both Joint and Service doctrines. Questions arise, however. To what extent can IO shape the battlefield? How susceptible is the US to IW, both at home and at deployed locations? This question entails everything from the adversary affecting our C2 information flow to national media influencing public opinion and driving foreign policy. Have we protected our own information infrastructure? Does the US have an IW early warning system? What are the indications and warning signs of an impending IW attack? To answer these and other questions, one must understand intricacies of the current information environment. The relationship of data automation even five years ago compared to that of today is analogous to a conventional bomb contrasted with a nuclear warhead. The explosion of connectivity (such as the Internet and Worldwide Web), data transmittal rates, networking, telecommunications, and dependence thereon, quite simply transformed military, political, and economic dynamics on a global scale.

Global Technology Trends

CATEGORY	**15 YEARS AGO**	**1996**	**5 YEARS HENCE**
PERSONAL COMPUTERS	THOUSANDS	400 MILLION	500 MILLION
LOCAL AREA NETWORKS	THOUSANDS	1.3 MILLION	2.5 MILLION
WIDE AREA NETWORKS	HUNDREDS	THOUSANDS	TENS OF THOUSANDS
VIRUSES	SOME	THOUSANDS	TENS OF THOUSANDS
INTERNET DEVICES ACCESSING THE WORLD-WIDE WEB	NONE	32 MILLION	300 MILLION
POPULATION WITH SKILLS FOR CYBER ATTACK	THOUSANDS	17 MILLION	19 MILLION
TELECOMMUNICATIONS SYSTEMS CONTROL SOFTWARE SPECIALISTS	FEW	1.1 MILLION	1.3 MILLION

Table 2. Global Technology Trends[1]

The Internet transcends national boarders…individuals of common interests form and operate within their own cyber-terrain. Deregulation, restructuring, and economic troubles also drove these changes, causing corporations to downsize and merge, eliminate forward-deployed offices and rely instead on "virtual" offices via interconnected networks and the Internet. When times improved, they expanded and upgraded their information infrastructures. Increasing network connectivity proved to be both a blessing and a curse. To the positive, it improved overall system reliability by providing backup programs. The detrimental aspect to increased network connectivity is that a weak link in one system can damage the entire network, exacerbating overall vulnerability. Few

individuals foresaw the exponential growth of the global Internet or the degree of reliance by technologically advanced nations. Hence, when systems were initially developed and subsequently linked, network security to the level needed today was not a prime consideration. Consequently, network owners are currently retrofitting to negate demonstrated vulnerabilities, even as adversaries continue to hone their own predatory skills.

Skeptics frequently underestimate the military's dependence upon civilian infrastructure. They claim that while the civilian infrastructure is vulnerable, "military systems are usually so isolated and uniquely programmed that there is little assurance they could be disabled in a military strike."[2] Recognizing the fallacy of this argument, the President signed EO 13010 on Critical Infrastructure Protection because, "Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."[3] EO 13010 established the PCCIP which combined efforts of federal, state, and local government officials with private sector CEOs and CIOs to address the issue of Information Assurance. The Commission was charged to assess the specific components of the infrastructure, identify vulnerabilities, and make recommendations to protect these national assets. This study examined: energy (electric power, gas and oil storage/transportation), physical distribution (railroads, highways, air traffic, maritime transport, and pipelines), banking and finance, information and communications (computers, software, satellite communications, etc.), and vital human services (water supply system, emergency rescue services, social security, and welfare).[4]

The US is arguably one of the world's most technologically sophisticated nations, among the most dependent on information infrastructures....and the most vulnerable. Stand alone, local area networks (LANs) rapidly evolved to what is now referred to as cascading information infrastructures at the DOD (DII), national (NII), and global (GII) levels. Most of our $6 Trillion economy relies on an estimated 125 million computers, associated networks, and satellite connectivity. These automated infrastructures have an estimated financial value of $23B, $500B, and $1000B, respectively.[5] According to the Commission, the US uses 42% of the world's computing power, 60% of the world's Internet assets, and operates on-line 200 million hours daily. It also determined the extent to which private and government functions depend upon information and communications. Specifically, 90% of large and 75% of small businesses have LANs, and the Federal government spends $40 billion annually on information technology.[6] Another significant observation concerned the eroding distinctions between DII, NII, and GII. Commercial ownership of a majority of the connected networks adds a further complication to the challenge of information protection. The US military, traditionally charged with defending continental borders of the United States, has no jurisdiction over the borderless cyberspace and little control over NII infrastructures upon which its forces depend.[7] For example, 95% of DOD communications use commercial backbones.[8]

The Secretary of Defense simultaneously tasked the Defense Science Board (DSB), a Federal Advisory Committee, to address Information Warfare-Defense (IW-D). The efforts ran concurrently and reached similar conclusions. The task force made 50 recommendations in its final report, 13 of which were deemed "imperative." Several recommendations are carryovers from previous DSB reports spanning the past 3 years,

indicating progress not yet made. The report noted the DOD employs more than 2.1 million computers, an estimated 10,000 LANs, and over 100 long-distance networks, used to support all facets of military operations.[9] Lack of progress in eliminating system vulnerabilities and increasing US reliance on these strategic infrastructures is a potentially disastrous combination. The most urgent recommendation contained in the Nov '96 report was that SECDEF "designate an accountable IW focal point." The second was that DOD should organize for IW-D by establishing "virtual organizations that draw on existing assets and capabilities." DSB suggested allocating approximately $3 billion to implement recommended fixes.[10]

The National Defense Panel (NDP) strongly agreed. Its December 1997 report contrasted likely antagonists and future threats (e.g., Information Warfare and WMD) with current DOD organizational structure and projected budgets. The NDP identified a major disconnect. Its overarching recommendation was to align our organization to best accommodate future threats and vulnerabilities. Using the Toffler analogy, the U.S. showed transition from an Industrial (Second Wave) to an Information (Third Wave) military posture.[11] The Executive Summary began with a warning, "Only one thing is certain: the greatest danger lies in unwillingness or an inability to change our security posture in time to meet the challenges of the next century." It concluded with an ominous statement, "If we refuse to change in a timely manner we could be fundamentally unprepared for the future, and put at risk the safety of future generations of Americans."[12]

A modicum of progress has been made towards resolving these shortfalls. DOD intensified its approach to both offensive and defensive aspects. As an example, in March 1998 Secretary of Defense Cohen proposed a new deputy assistant secretary for

IO within the extant structure of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD/C3I). This new position would oversee two directorates: one for information assurance and the other for offensive information operations. According to Barry Collin, senior research fellow at the Institute for Security and Intelligence, "It's the most exciting revelation to date on the information operations front. It shows the maturing nature of information operations as an offensive tool, which is new. It's going to be taken seriously."[13] Meanwhile, vulnerabilities persist.

Notes

[1] Defense Science Board, *Task Force on Information Warfare-Defense*, November 1996, Section 2.3.

[2] *Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance*, 2nd Edition, Jul 96, by Joint Staff, pg 2-15.

[3] Michael A Dornheim, *Bombs Still Beat Bytes*, Aviation Week and Space Technology, January 19, 1998.

[4] Executive Order 13010, *Critical Infrastructure Protection,* July 1996.

[5] Remarks by Stevan Mitchell, Commissioner PCCIP, at DOD Worldwide Antiterrorism Conference, August 21, 1997, pg 10.

[6] Briefing, *Information and Communications Sector: The Nation's Central Nervous System*, Nancy J Wong, PCCIP Commissioner

[7] Remarks by Stevan Mitchell, Commissioner PCCIP, at DOD Worldwide Antiterrorism Conference, August 21, 1997, pg 10.

[8] Remarks by Stevan Mitchell, Commissioner PCCIP, at Howard University's JFK School of Government, September 20, 1997, pg 2.

[9] Defense Science Board, *Task Force on Information Warfare-Defense*, November 1996, Duane P. Andrews, Chairman, Section 2.3.

[10] Ibid., Section 7.

[11] Alvin Toffler, *War and Anti War,*, Warner Books Inc, NY, 1993.

[12] Executive Summary, National Defense Panel Report, December 1997.

[13] Robert Brewin and Heather Harreld, *DOD Adds Attack Capability to Infowar/Move Follows Latest Round of Hacks,* Federal Computer Week, March 2, 1998.

Chapter 3

Information: The Alpha and Omega

Information is power. In the Information Age, proponents of Star Trek-like IW must consider the vulnerability and susceptibility of the media, the American public, and our policy makers to information applied by adversaries to wage deception and psychological operations against the US. Adversaries expertly manipulate the media, leveraging them against the US' well-publicized lack of tolerance for American bloodshed or ill treatment of a 'defenseless' people. They wage Information Warfare against the US in the form of PSYOPS, altering perceptions and the will of the American public, with the aim of affecting American foreign policy. For decades, terrorists adroitly exploited the media to state their case to the general public or to amplify the terror of their attack. In the Information Age, adversaries refined this stagecraft into a fine art, actively courting the power of the press to sway world opinion. The press willingly obliges.

Examples abound: Iraq, Somalia, Haiti, Rwanda, and Bosnia, to name a few. Saddam Hussein deflects attacks from strategic sites, such as command posts, by collocating civilians as human shields. He stages anti-American riots in the streets of Baghdad covered by CNN, bolstering domestic morale as well as making a global statement. In Somalia, Aideed and his low-tech insurgents waged info war and soundly defeated the US. Mimicking Sadaam's techniques, Aideed transformed the Mogadishu

Hospital into a strong point for militia operations realizing that the UN would not target the facility. He was a master of manipulation, deception, and staging events conveniently accessible for media coverage. Aideed was able to successfully manipulate peace initiatives and cease fires to deprive the international force of a political rationale to militarily oppose his political maneuverings.[1] Images of a dead, naked American soldier gleefully dragged through dirty Somali streets trumped our technologically superior military might. The adage, "One picture is worth a thousand words" gains new significance in the Information Age, highlighting a major American vulnerability. The History Channel's presentation of "The Power and the Image" succinctly admonished, "Control the images on the screen before they destroy you!"[2]

"All the world is a stage." In the Information Age, the media certainly takes center stage. Thanks to the media, not much passes unseen. For example, the entire world watched and learned military lessons from DESERT SHIELD and DESERT STORM. That the US mustered daunting force-on-force was a point missed by few, friends and foes alike. These operations explosively proclaimed America's conventional military might, strongly discouraging adversaries from engaging the US in similar conflicts. That this conflict heralded the age of IW was also widely noted. Sun Tzu correctly advises warriors to view battles from the adversary's perspective, to determine inherent strengths and weaknesses (physical and psychological), and presume those weaknesses to be prime targets in future conflicts. Just as the United States possess lethal and effective conventional forces, numerous nations and non-state actors are intently developing the art of IW.

Notes

[1] Rick Brennan and R. Evan Ellis, *A Case Study of Somalia,* April 18, 1996 SAIC Project Number: 03-9847-000 SAIC Document Number: 96-6960 & SAC Prepared for the Office of the Secretary of Defense, Net Assessment.

[2] *Power of the Image*, History Channel broadcast.

Chapter 4

They…..RRR Here! But Who Are They?

The form of any war—and it is the form which is of primary interest to men of war—depends on the technical means of war available.

—Douhet[1]

Simple statement…the US is not at peace. The Cold War is dead but an Info War, the very same war that killed the Cold War, still rages. Its prime characteristics—stealth, manipulation, and deception—are so subtle, the American public is manifestly and dangerously unaware. Information technologies are inexpensive and easily obtained, originating points of attack are difficult to locate, perpetrators hard to identify, damage of times difficult to detect. Recognized as strategic targets, elements throughout our NII and DII are attacked daily. NII targets frequently hit include Public Switched Telephone Networks (PSTN), financial institutions, and transportation control points, all obviously crucial to employment of USAF forces. Attacks on the DII are also prevalent. The GAO estimated 250,000 attempted penetrations of unclassified DOD systems during calendar year 1996.[2] The Defense Information System Agency (DISA) estimates 65% of DOD unclassified systems are vulnerable to penetration.[3] Only a small fraction of penetrations are detected and a smaller percentage actually reported. Unclassified systems, usually less stringently protected than classified counterparts, pose tempting and lucrative targets.

However, disrupting, corrupting, or otherwise impeding the flow of unclassified data can severely impede military operations.

In February 1998, the DOD came under a widespread, structured, and systematic attack on unclassified computer systems. Over at least a 2-week period, perpetrators targeted 11 sites belonging to both the Air Force and Navy. Most of the attacks concentrated on domain name servers (DNS) which transmitted unclassified but still sensitive defense information such as logistics, personnel, and payroll data. It might be helpful at this point to quantify the seriousness of such a security breach. In compromising a DNS, a perpetrator could potentially access multiple passwords, preclude message delivery, and even alter the content of messages…unbeknownst to the intended recipient. DOD scrambled to assess the damage and identify the perpetrator(s), both incredibly challenging objectives. One author observes, "The electronic intrusions, which were detected early last week, serve as a stark reminder that despite its warfighting prowess, the nation remains highly vulnerable to assaults on its ever-growing information infrastructure."[4] According to an article by the Associated Press, Deputy Secretary of Defense John Hamre speculated that attacks have been aimed at inserting hidden trapdoors into the system for future surreptitious entry.[5] Aviation Week carried an article on offensive IW not more than 2 weeks prior to this series of intrusions. The author supposes, "In some future international crisis, communications switching stations may be primary targets for offensive attacks by computer hackers serving the US military. These sites provide several needed elements for getting 'inside an opponent's mind' as some US officials describe the task of penetrating foreign computers to read communications

traffic."[6] In retrospect, this article seems almost prophetic in its timing and ironic in that the US was the victim rather than the perpetrator, as the author presumed.

Two abysmal footnotes to this attack must be mentioned. The first is identification of the perpetrators. Some analysts initially speculated that this attack might be associated with the US build up in the Middle East. Others assessed the attack as teenage hacking…highly skilled…but amateur "cyber-kids", nonetheless. The probes lacked the intensity of a focused, professional attack. As it turns out, teens were indeed the culprits. The second sobering observation was DOD's lack of preparation to respond effectively and expeditiously. In absence of a clearly delineated IO structure within DOD, the center of gravity for rallying a response fell to the Joint Staff/J39, an organization charged with policy development, not running defensive operations. Recall the cliché, "If you can't stand the answer, don't ask the question." The US does not have the luxury of avoiding a poignant question here…"If two teenagers can singularly grip the attention of DOD and cause havoc regarding information defense…how will the US respond to a covert, more insidious, purposeful attack?"

Potential adversaries, plentiful as targets within our infrastructure, are multiplying: amateur computer hackers; "professional" non-state actors (e.g., terrorists); organized crime (e.g., drug cartel or Mafia); the traditional adversarial nation-state; and even disgruntled domestic employees. According to a DOE and NSA estimate, 120 countries are developing IO capabilities.[7] China, for example, intently focused on IO, recognizes that on battlefields of the future, "information and Information Technologies (IT) will be the dominant factors." The BBC Summary of World Broadcasts in Aug 1996, carried an item which announced China's development of the Military Strategies Research Center

focused on IO, and translated an article published in the Chinese paper, "Jiefangjun Bao'on 21 May, '96. An extract of same follows:

> After the Gulf War, when everyone was looking forward to eternal peace, a new military revolution emerged. This revolution is essentially a transformation from the mechanized warfare of the industrial age to the information warfare of the information age. Information warfare is a war of decisions and control, a war of knowledge and a war of intellect....The all conquering stratagems of Sun Zi more than two milleniums ago, such as 'vanquishing the enemy without fighting' and subduing the enemy by 'soft strike' or 'soft destruction' could finally be truly realized under today's technological conditions.[8]

In an August 1997 article, Wang Xusheng of the PLA Academy of Electronic Technology, proposed a six step plan to build an information-age China:[9]

> 1. Build an information network architecture for use by civilian and military sectors in peace and war. Accelerate pace of modernization of information-age armed forces.
>
> 2. Strengthen the training of capable people. Advancement will depend on people who understand high technology.
>
> 3. Give free rein to the market's driving power. There must be governmental administration, policy making, general planning, joint construction and coordinated development, thus allowing networks to serve both market and battlefield.
>
> 4. Adopt new technology. Integrate Information Technology with other technologies to increase the efficiency of information application.
>
> 5. Enhance survivability of information networks. System should have good anti-reconnaissance, anti-bugging, survivable capabilities, extremely flexible, well-concealed, and able to operate under a wide variety of conditions. China should also establish a military information defense network.
>
> 6. Strengthen legislation concerning information and strengthen information administration. Infosec is an important mainstay of national defense and the safeguard of national security. This is an extremely important step towards building the national economy and the national defense within the context of a legal system.

The author concludes with the observation, "We must use the power of information to promote great strides in the national economy's 'market' and ensure that we hold the initiative on the 'battlefield' of the military struggle."[10]

The Russians are experts in IO, and can claim operational experience dating back to the 1920's when Felix Dzershinsky founded the Cheka which later evolved into the KGB. It is important to remember that, as discussed above, IO encompasses many techniques and tactics other than computer penetration or ADP manipulation. The Russians employed "active measures" on a global scale, literally. This benign term encompasses: forgeries, deceptive information, rumors, staged protests, use of front organizations, blackmail, bribery, and manipulation of the media. Some analysts estimate that during the height of the Cold War, the Soviet Union spent $3 billion annually on active measures. Stanislav Levchenko, a former high ranking KGB official who defected to the United States, warned that, "By weakening or destroying the consensus within a free country, active measures do much more harm than classical espionage. In the West, few people understand this concept."[11] One example of media manipulation that occurred in 1979 bears repeating because of its relevance today, and potential application by contemporary adversary nations such as Iraq. A French journalist, Pierre-Charles Pathe, was exposed after serving as a media mouthpiece of the KGB for 19 years. During this time, he became a highly respected member of the media and leveraged great influence in both governmental and industrial circles. When his complicity was discovered, he was tried, found guilty and sentenced to 5 years in prison.[12]

Regarding the technologically advanced computer warfare, the Soviet Union was among the leaders there, as well. One of the first highly publicized instances of computer

penetration, detailed in Clifford Stoll's book, "The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage," was tracked back to Bulgarian KGB.[13] Despite current economic woes, Russia continues an active R&D program in the area of IO and is among those countries attempting to weaponize computer viruses. Russia recently institutionalized its efforts by creating the obliquely titled, Federal Agency for Government Communications and Information.[14] This analysis doesn't necessarily postulate an immediate IO threat posed by the Russians. But it does recognize their history of in-depth expertise in the IO field and serves as a reminder that once learned, such lessons learned ought not be forgotten.

Recognizing vulnerabilities inherent in the Information Age, the USAF is developing and conducting exercises to determine the severity of the IO threat and our ability to respond. The first such groundbreaking exercise, ELIGIBLE RECEIVER, was concluded in June 1997. This no-notice exercise was a "first" in several respects. ELIGIBLE RECEIVER brought into play, via both script and real action, all elements of IW: deception, EW, PSYOP, information attack, and physical attack.[15] The scenario included an adversary PSYOP campaign making efficient use of the US news media, scripted terrorist attacks on public power and communications, actual "hostile" IW attacks on DOD communications and computer infrastructures, and extensive E-mail spoofing to confuse the Blue Team. It demonstrated accessibility of US databases to adversary intrusion, difficulty national-level organizations (e.g., DoJ, NSA, and DOD) experienced differentiating a normal outage from an actual attack, and even recognizing database compromise once that had occurred. Also highlighted was the cumbersome coordination process at the national-level which slowed the process of sharing

information relative to an ongoing IW attack, and impeded efforts to recover lost data, while protecting as yet unaffected systems.[16]

The major benefits resulting from this exercise were the identification of what didn't work and operational degradation resulting from IO attacks. In several instances, successful IO attacks did, in fact, delay deployment of US forces. Coordination among federal agencies was painfully slow, taking days rather than hours. DOD lacked an organization to coordinate notices of attack, responses as situations deteriorated, and efforts to reconstitute. This responsibility fell to the exercise "Joint Staff" by default. Little coordination occurred between military and private companies, impeding the eventual recognition of a coordinated attack on the infrastructure, vice random accidents. Organizations involved demonstrated minimal IO awareness. In most instances, system administrators failed to detect successful, real-world, physical computer penetrations. On the offensive side, the exercise CINC experienced great difficulty in obtaining approval to implement IW operations. Furthermore, most of the presumed ADP-related offensive IW weapons are so sheathed in secrecy, they were simply unavailable for exercise play. This begs the question of the utility of such weapons, especially when juxtaposed against the theory of "Train in peace as you would execute in war." One of the significant lessons learned from this exercise was the need for an IO cell integrated into the CINC's warfighting staff. This led to an imaginative and thought provoking question, "What might be the composition of an IO Dream Team and what would it contribute to a warfighting CINC?"

Of primary importance, the IO Dream Team must be joint. It would consist of personnel skilled in the various aspects of IO much like the Joint Command and Control

Warfare Center, now manned by these assorted skills, most recently incorporating PSYOPS expertise. Legal representatives must also be included within the IO cell to clarify rules of engagement as pertains to application of IW. Public Affairs personnel must also be intimately involved in both planning and execution of IO. The IO cell would be charged with developing an IO campaign, supporting traditional air, land, sea, and space forces…certainly. However, this team would also recognize and resist the inherent, restrictive tendency to apply new weapons technology exclusively to established war fighting doctrine as a mere force multiplier. This is reminiscent of the tension in WW II between subordinating airpower to Army commanders for close air support of ground forces, as opposed to maintaining airpower as its own entity and applying air assets to a new mission….strategic bombing.

The team must literally think like the enemy, rather than the usual US inclination…presume the adversary will react in a typical Western fashion. These individuals would really know the enemy…how he thinks; anticipated response to external stimuli; his predisposition on religious, social, cultural, and economic issues; degree of popular support; his particular strengths and weaknesses. To obtain these insights, the Intelligence Community must reinvest in and reinvigorate emphasis on geopolitical and economic analysis. These areas suffered from cutbacks in recent years, as organizations chose to protect the more technical and military-related fields. With this information, the IO cell could devise a penetrating and effective IO campaign. General Patton exemplified this approach in his battles against Field Marshall Rommell. Why was Patton so successful? One scene in the movie "Patton!" makes the point…while

gazing off at a distance, the general crows, "Rommell, you poor bastard, I read your book!"

Ideally, IO officers would be trained in proven IO techniques employed during WW II. The 1930's and 1940's were replete with technological innovations such as radar, expanded range of radio waves, advances in cryptology and resulting impact on Signals Intelligence, and innovative methods of deception. The Cold War birthed "active measures" and techniques of meaconing, intrusion, jamming, and interception (MIJI)...perhaps experts within the emerging Russian democracy might provide that training as an initial step towards sharing IO methodology with allies. Or, perhaps those who've already defected could impart that hands-on expertise. The wise student chooses to learn from the experts and in the Cold War, the Russians were the best. To meet the challenge of today's information war, we could do well to study and learn from contemporary adversaries such as Iraq's Sadaam Hussein and Somalia's Aideed.

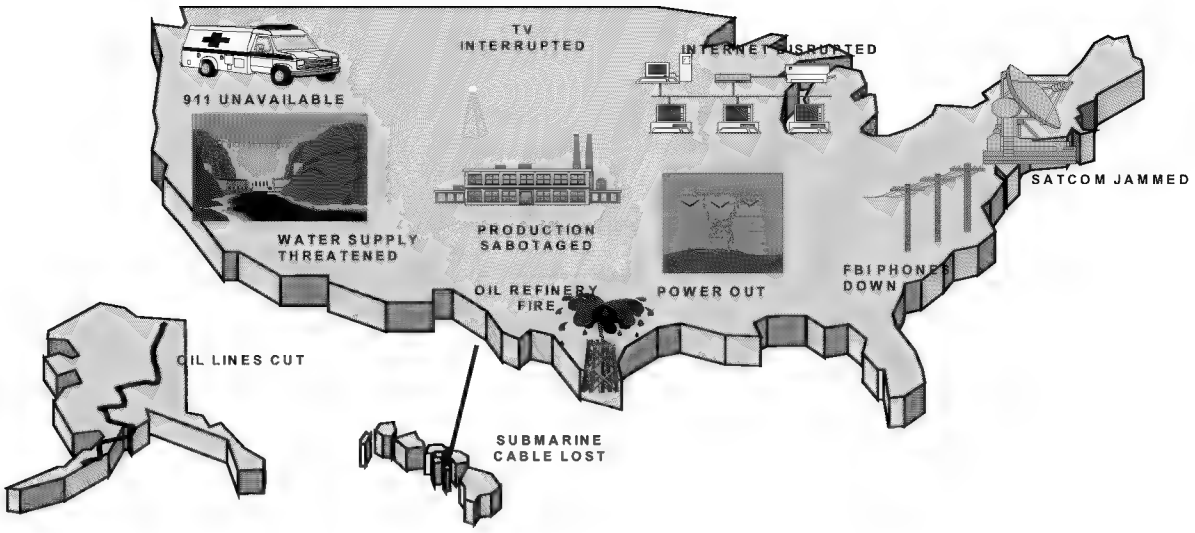

Figure 2. Disruption Map

Several questions were raised in the discussion at the conclusion of exercise Eligible Receiver. How to distinguish a hostile attack from amateur perpetrator and single event from a planned campaign? The above chart illustrates the complexities in making this determination. How do DOD and DoJ agencies legally share data on computer attacks? How can interagency coordination be expedited from hours to minutes? What agency should function as a central point for detecting, alerting, and responding to information attacks? How can DOD effectively develop, and retain, skilled system administrators? Should DOD establish a Commander in Chief for IO? If so, who? An even more imposing question…***when*** will DOD stand up an organization to anticipate, respond to, and reconstitute from an IW attack? ELIGIBLE RECEIVER spotlighted this weakness and as the two teenage hackers painfully demonstrated 8 months later…it's still not fixed. Time's a wastin'.

Notes

[1] Douhet, *The New Form of War*, Air War College Strategy, Doctrine, and Airpower, Book II, Air University Press, August 1998, pg 4.

[2] Remarks by Stevan Mitchell, Commissioner PCCIP, at Howard University's JFK School of Government, September 20, 1997, pg 2.

[3] Defense Science Board, *Task Force on Information Warfare-Defense*, November 1996, Section 2.3.

[4] *Pentagon Looks for Answers to Massive Computer Attack*, Defense Information and Electronics Report, February 13, 1998.

[5] Suzanne M. Schafer, *Hackers Invade Pentagon Computers*, Associated Press, February 26, 1998.

[6] *Attack Software Plays Key Offensive Role*, Aviation Week and Space Technology, January 19, 1998.

[7] *Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance*, 2nd Edition, Joint Staff, July 1996, pg 2-111.

[8] Anthony Cajigas, *The Secret Battlefield, Computer Warfare Contingencies II*, pg 2 nick_dav@ix.netcom.com.

[9] Wang Xuaheng, et al, *China: Information Revolution, Defense Security*, Beijing Jisuanji Shijie (China Computerworld), August 11,1997.

[10] Ibid.

[11] *Active Measures Key to Soviet Discrediting Campaign,* Washington Times, May 23, 1985.

[12] Ibid.

[13] Clifford Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage,* NY: Doubleday; 1989.

[14] George Stein, *Jane's Special Report: US Information Warfare*, Jane's Information Group, Alexandria, Va. 1996, pg 22-26.

[15] Kenneth D. Bryan, *Shop Talk: PACOM Team,* Cyber Sword, Vol. 1, Number 2, pg 38-39, Fall '97.

[16] Whit Peters and Richard Marshall, Briefing *Defensive Information Operations*, October 18, 1997, USAF Information Operations Conference.

Chapter 5

Sand Is Not A Good Foundation Make!

> *The state must make such disposition of its defenses as will put it in the best possible condition to sustain any future war. But....these dispositions for defense must provide means of warfare suited to the character and form future wars may assume.*
>
> —Douhet[1]

AF policy focuses today on concepts such as Full Spectrum Dominance, Dominant Battlespace Awareness, "find, fix, track or target anything that moves on the surface of the earth."[2] Pretty presumptuous concepts. Joint Vision 2010 also sets lofty operational strategies: dominant maneuver, precision engagement, focused logistics, and full-dimensional protection. In a speech at the 1997 AFCEA convention, Admiral William A Owens, USN (Ret.), former vice chairman of the JCS, envisioned all-encompassing sensors enabling the US to view in detail adversary movements in any theater of battle.[3] The enemy would presumably acknowledge his infallibility due to our all-seeing sensors and voluntarily acquiesce to US desires. The accompanying US strategy would seem to be, intimidate by information. In addition to recklessly assuming inviolability of our reconnaissance and surveillance technology, this approach seriously underestimates the adversary's religious or revolutionary fervor. Admiral Owens illustrates the frequently demonstrated inability of the US warfighter to think like the enemy and the persistent

proclivity to expect the enemy to respond as would US commanders. This is a proven flawed strategy and a lesson US warfighters seem unable to learn.

A similar futuristic concept is promoted in a RAND study, "The Virtual Combat Air Staff: The Promise of Information Technologies."[4] This book postulates a "virtual" combat air staff in the years 2010-2020, a staff in which most members are geographically removed from the decision making nucleus and out of harm's way, hence the term "virtual." Technology would enable deployed forces to reach back to numerous functional experts, accessing more near-real-time data than would otherwise have been available at deployed locations. Reach back would improve the quality of products, enabling the commander to maintain battlespace awareness but with smaller staffs on hand. Although "The Virtual Combat Air Staff" presents an interesting view of combat staffs 13 years hence and skillfully assimilates anticipated technologies into planning and executing air campaigns, part of the argument seems missing and some assumptions questionable.

Several questions arise concerning the personnel and organizational aspects of the "virtual" combat staff. Will commanders be comfortable with the geographically separated aspect of "virtual" staffs? Dislocation is, as the argument goes, the essence if "virtuality." Judging from the difficulty in current proposals to remote intelligence collection from the Korean peninsula, I would suggest...not, unless the DOD makes tremendous advances in information assurance. The authors don't totally disregard IO vulnerabilities. The issue is raised fleetingly but treated superficially and optimistically, casting doubt on their understanding of the complexities and challenges in protecting US information and supporting systems. Several examples support this observation. A

section in chapter three, "Potential Operational Needs," addresses numerous technological advances in detail but gives a one-line, passing reference to the need for "Adaptive safeguards--to assure protected, uninterrupted C4I" and continues, "it does not appear that any intrinsic [technology] show stoppers lie in the path ahead."

Another concern is surfaced regarding, "jamming of links and attacks on the integrity of databases" but is later countered with, "Jamming and information security issues have been adequately addressed in the past...It seems reasonable that technology will continue to advance in areas that will work to provide secure, anti-jam communications."[5] Omission of vulnerabilities to cyberwar was especially apparent in the operational scenario of chapter six, used to demonstrate theories and technological innovations put forth in earlier chapters. Finally, projections of, "almost unlimited access to command authorities and fielded forces via worldwide communications" and, "The future of the information age promises unlimited access to means for communications." seem overly optimistic. This unbalanced enthusiasm for cyberwar is readily recognized by skeptics and actually detracts from efforts to convince military personnel on operational applicability of IO.

Upon what do these concepts depend? Technology. Why the emphasis? Global deployment of US forces and increasing number of military operations other than war (MOOTWs), coupled with a decreasing DOD budget and downsized military created a gap in US force projection and warfighting capabilities. Technology will *supposedly* close that gap. What underlying foundation is absolutely fundamental? Information—the assured availability of friendly data (termed "Information Assurance") and knowledge of adversary intentions, movements, and status of forces (i.e., intelligence).

> Recognizing improvements in technology and information systems…full spectrum dominance allows joint forces to prevail across the range of national military strategy from peacetime engagement to deterrence and conflict prevention, to fighting and winning in combat.
>
> AFDD 1-1[6]

Strategies laid out in AF *Global Engagement* and *Joint Vision 2010* are based on several presumptions. First, our C2 systems are interoperable and fully capable of transmitting data among US and Allied forces. Second, intelligence collection, production, application, and dissemination are sufficiently robust to collect against any required target, employing both technical and human intelligence (HUMINT) resources, as appropriate. Third, US wartime data flow will be impervious to Information Warfare attacks. And fourth, services will recognize, exploit, integrate, and apply IO capabilities in future operations.

All four presumptions are currently flawed. First, our C2 systems are not yet interoperable among DOD forces, and certainly not with Allied systems. The National Defense Panel also recognized this shortfall, "we must move rapidly to the next level of "jointness" among uniformed services: full commonality of US military information systems. This commonality must be interoperable with the information systems of our allies as well, if we are to reap the advantages of coalition operations." The report further specified that the US should develop greater interoperability with allies in the following areas; doctrine, training, operational techniques, and R&D.[7] Furthermore, we have not completed protocols for sharing what information, with whom, and how…and are only beginning to view this from an IW perspective.

Second, while intelligence might provide data to find and target most items on the face of the earth (but certainly not all, as we saw in Iraq), intelligence systems can still be

deceived by dummies and decoys; thus, the issue becomes one of targeting the right item. Also, air and space-based systems cannot supplant intelligence provided by the guy-on-the-ground. HUMINT adds a unique and essential dimension to the intelligence product and will have an even larger role in the Information Age. As such, the DOD HUMINT effort must certainly be strengthened to better support both tactical and strategic applications. IO also introduces an entirely new paradigm affecting the entire intelligence cycle. The US Intelligence Community must identify and collect IO-related essential elements of information, generate and apply timely analytical products, and establish an Indications and Warning system to anticipate IO attacks. Finally, we must develop the tools and methodology to instantly detect penetration, quickly move to block exploitation, and ascertain damage inflicted an info attack (i.e., equivalent of kinetic "bomb damage assessment") waged both against us and against our adversaries. These efforts are only now beginning.

Third, the US should not plan combat operations based on an information friendly environment. IW is likely to become a prominent feature of future wars. As such, projections of adversary offense and defense operations should include the range of IW options available to the adversary. As stated earlier, an estimated 120 countries are pursuing IO capabilities. Many are gathering data on US DOD and other critical information systems and are devising methods of attack.[8]

Forth, services are just recently beginning to incorporate IO in exercises, subsequently experiencing and understanding the results of IW attacks. This aspect highlights the defensive, i.e., the need to protect information. It does not yet allow teams to exercise offensive IO weapons which are still shrouded in Black programs. As this

subject area is so new, services lack the experience of planning and executing well rounded IO operations. As in the early days of airpower, some of IO's most stringent critics are among DOD's upcoming senior leadership. Some critics even walk the halls of military academia. Lt Gen Buckholtz, director for command, control, communications and computer systems, Joint Staff (J-6), warns,

> Awareness [of the IW threat] is singularly the biggest problem we have. We've got to get folks up to speed on this....The problem is getting warfighters to really understand that this is every bit as significant as some enemy bomber that comes in and does something to the United States. It's just that they've been raised on tanks and planes. Getting the warfighter who has been under fire many times to agree that networks are better than [weapons] that shoot is tough. There's a big mind-set you've got to overcome.[9]

Tensions in the Taiwan Straits during 1995 seemed to substantiate futurist projections of a "virtual" staff. Vice Admiral Cebrowski and Rear Admiral Nutwell both agree that information networks have, in themselves, become combat systems. Most command information exchanges during this crisis situation were based on video teleconferences and electronic mail--which enhanced the speed of command and situational awareness, making communication "light years better than phone calls and AUTODIN messages that once took hours or days."[10] Keeping the situation in context, the US Navy successfully applied this technology because the application was not aggressively countered. Ten years hence, IO offensive efforts are likely to be as robust as the technology that would make possible "virtual" combat staffs. The result, an obvious reduction the efficiency of the "virtual" staff, unless major steps are achieved and implemented in the field of IO defense. In actuality, 1995 tensions in the Taiwan Straits demonstrates the need for a balanced assessment of technology and its application in the Information Age, recognizing both capabilities as well as potential limitations.

Notes

[1] Douhet, *The New Form of War*, Air War College Strategy, Doctrine, and Air Power Book II, Air University, November 1998, pg 3.

[2] *Global Engagement: A Vision for the 21st Century Air Force*, pg 1.

[3] *Military, Industry Partners Grab Information Systems' Brass Ring,* Signals Magazine September 97, pg 91.

[4] Arthur Huber, et al, *Virtual Combat Air Staff: The Promise of Information Technologies*, RAND, 1996, pg 96.

[5] Ibid., pg 56-57.

[6] Air Force Doctrine Document (AFDD) 1-1, *Air Force Basic Doctrine*, September 1997, pg 36.

[7] *Transforming Defense: National Security in the 21st Century*, Report by the National Defense Panel, December 1997, pg 14, 32.

[8] Jason Sherman, *Infowar? What Kind of a Defense?,* Armed Forces Journal, August 1997.

[9] Ibid.

[10] *Military, Industry Partners Grab Information Systems' Brass Ring*, Signals Magazine, September 1997, pg 91.

Chapter 6

Horns of the Dilema—What To Do?

> *The defense of our commercial and military information architecture will be critical and will allow us to protect our forces and our platforms from the enemy's reconnaissance efforts. New means to protect information systems and identify the origin of cyber-attacks must be the highest priority. Today, we are vulnerable.*
>
> —National Defense Panel[1]

The US military faces a conundrum. On one hand, the DOD relies heavily on technological advances in the Information Age in response to defense challenges and global commitments of the 21st century. For example, DOD leverages technology to offset reductions in manpower. On the other hand, inherent vulnerabilities of global connectivity could be our nemesis. DOD faces a dilemma. Is this dichotomy incongruous? If not, what must be done to negate the variance? Differences can be resolved and the DOD can establish a foundation firmer than sand, but only with significant resource investment and dedicated, bold, and conscious effort. How? Prudence dictates the US achieve strong, demonstrable IO deterrence as soon as possible. Douhet recognized the urgency for bold action and cautions,

> To break away from the past is disturbing...if we have a tendency to deviate as little as possible from the beaten path, we will find ourselves diverging from reality, and we will wind up far removed from the realities of our time.[2]

Information Assurance…the key ingredient to credible IO deterrence. Information Assurance…the certainty of information readiness, reliability, and continuity. Information Assurance…that firm foundation upon which we can base Air Force doctrine with some realistic expectations of success. We've defined it and recognize its importance. Now, what must we do to obtain Information Assurance? The steps described below focus on DOD challenges. However, both DSB and PCCIP reports strongly emphasize most of these same steps must be mirrored by cooperative efforts between commercial and government organizations at the local, state, and national-levels.

First, the DOD must secure vital information systems and then convince adversaries that these systems are, in fact, resilient. This involves calculated risk management: identifying, protecting, and making robust only those information systems and processes most critical to national defense, an approach similar to Continuity of Government operations undertaken during the Cold War. The DOD should identify the most crucial databases, the corruption or destruction of which could severely impede military operations. It should be noted, these databases will not necessarily be exclusively classified. DOD should then either maintain duplicate, backup systems or increase automated defenses for these systems. Second, we need a viable Indication and Warning (I&W) capability to anticipate, preclude or that failing, ameliorate effects of IW attacks. This entails developing an I&W methodology and establishing a joint 24-hour center to analyze I&W indicators, publish warnings, coordinate data on attacks in progress, assess the damage, and monitor efforts to reconstitute. Geographically focused, emergency response teams would complete the I&W capability. Third, we must be able to respond

to an information attack in kind, when necessary, and clearly convey to adversaries fact of that capability and a willingness to apply it.

The fourth element lies with the American judicial system, but affects daily application of DOD IW policies and procedures. Laws must be modified to reflect offensive and defensive aspects of the Information Age and procedures streamlined to expedite data sharing among DOD, DoJ, and commercial organizations. This is admittedly a difficult area to negotiate, from a legal perspective. Civil liberties, such as freedom of speech and even freedom of assembly, are intertwined on the Internet with extremist groups sharing data on how to hack computers and build bombs. On the other hand, current legal restrictions prohibit looking beyond one computer hop without a court order. This severely curtails DOD investigative agencies in their attempts to detect who is waging an IW attack. Additionally, punishments for convicted hackers must be swift and sufficiently severe to serve as a deterrent. Current punishments simply do not deter, nor do penalties reflect the severity of resulting damage. For example, in 1997, a Swedish hacker jammed 911 lines in Miami, diverted emergency calls, and accessing the public telephone system, generated 60,000 unauthorized calls. The penalty? He was tried in Sweden as a juvenile and fined $345. It should be noted also, that many countries have no laws whatsoever pertaining to computer crime.[3] A fifth and final element mentioned here requires changes in the design specifications for ADP systems. We must stop building systems with internal weaknesses, making them vulnerable to malevolent exploitation and manipulation. Designing more secure systems will probably increase the end cost but is much more pragmatic than fixing system vulnerabilities later, assuming we detect their existence. Granted, some of the above mentioned actions are difficult, if

not impossible, to accomplish with today's technology. Nonetheless, these shortfalls point the way to needed R&D investment. Taken together, these components comprise the principle of deterrence applied to what is now known as Information Operations or the "the fifth battlespace domain."

A final element must be addressed within the international arena…that of IW. The Law of Armed Conflict should be thoroughly reviewed in the context of IO to resolve several basic issues. Does IW constitute an act of war? Is response in kind considered fair play? Should the international community define a level of acceptable damage generated by IW? Should it move to outlaw IW, using a vehicle similar to the Nuclear Test Ban Treaty? Since IO is already conducted daily and IW will most certainly be conducted in war, would a Ban be successful in pushing Pandora back into her box? Would such an approach merely disadvantage signatories and benefit adversaries who don't play by the rules? On the other hand, should the US even surface such questions to the international arena? One thing is certain…

> The United States may be faced with an adversary who seeks to offset United States' advantages by using asymmetric means and threatening the use of chemical and/or biological weapons, information attacks, terrorism, urban warfare, or anti-access strategies. Thus, America must quickly seize the initiative from the aggressor…a new way of looking at conflict is emerging.
>
> AFDD 1-1[4]

Notes

[1] *Transforming Defense:National Security in the 21st Century*, Report by the National Defense Panel, December 1997, pg 44

[2] Douhet, *The New Form of War*, Air War College Strategy, Doctrine, and Airpower, Book II, Air University, November 1998, pg 27.

[3] John T Correll, *War in Cyberspace*, Air Force Magazine, January 1998.

[4] Air Force Doctrine Document (AFDD) 1-1, *Air Force Basic Doctrine*, September 1997, pg 42.

Chapter 7

Who's On First? What's On Second?

Like supercharged electrons, organizations throughout DOD are scrambling for IO-related projects. Projects, contracts, working groups proliferate but under no central guidance and with no set methodology to share lessons learned. The skeptics are correct, to a certain extent. "IO" is the political emphasis *de jour*...and, funding is available for affiliated projects. But, the threat is real and organizations are reacting. The following initiatives illustrate the plethora of activity but are not inclusive, by any means. HQ Air Intelligence Agency (AIA) is the parent organization for 67 IW, the largest IO wing in the Air Force, and the AF Information Warfare Center (AFIWC). The AFIWC synthesizes a multitude of specialties (e.g., engineers, pilots, intelligence, and scientists), reflecting the diverse nature of IO. AFIWC, in turn, is parent to the AF IW Battlelab and the AF's Computer Emergency Response Team (AFCERT). Electronic Systems Division (ESD) and AFIWC co-chair an IW Technology Planning Integration Process Team. 609 IW squadron, subordinate to HQ Air Combat Command (ACC), assists CINCs in both offensive and defensive IO missions. The newest AF organization is the Air and Space C2 Agency at Langley AFB. The Navy implemented its Navy Information Warfare Activity (NIWA), focusing on long-term and budged affiliated aspects of IW, and the Fleet Information Warfare Center (FIWC) to provide current IO support to

deployed forces. The Army most recently initiated its Land Information Warfare Agency (LIWA). DIA leads the effort to develop an Indication & Warning methodology for IW and also leads an interdepartmental IW Threat Working Group. ESD's IW Division selects, installs, sustains base information protect products. AFCC is active in AF-wide information protect efforts and chairs the AF C4I Panel. AF/XOI chairs the Information Dominance Panel. Academia and defense contractors are also heavily involved in IO initiatives.

The Joint Staff J3 and J6 are heavily involved, as are other Joint organizations. The Joint Command and Control Warfare Center (JC2WC), collocated with HQ AIA and AFIWC, engages in a plethora of IO activities ranging from modeling and simulation to assisting theater CINCs plan and execute C2W and EW in both exercises and real world contingency operations. The Joint COMSEC Monitoring Activity (JCMA) monitors DOD telecommunications and automated information systems to identify vulnerabilities and recommends countermeasures and corrective actions. JCMA also supports both exercises and real world operations. The Joint Spectrum Center (JSC) ensures effective use of the electromagnetic spectrum and is the DOD focal point for spectrum supremacy aspects of Information Warfare. The Joint Warfare Analysis Center (JWAC) provides the Joint Staff and Unified Commands effects-based, precision targeting options for selected networks and nodes. The Joint Battle Center (JBC) provides combatant commands at the joint task force (JTF)-level an ability to experiment with and assess combat applications of Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR). The Joint Communications Support Element (JCSE) provides contingency and crisis communications to Unified Commands, Services,

Defense Agencies, and non-DOD Agencies (e.g., State Department, FEMA, NATO, and UN). The Joint Warfighting Center (JWFC) assists the CJCS, CINCs, and Service Chiefs in preparation for joint and multinational operations through conceptualization, development, and assessment of current and future joint doctrine, and application in training and exercises. Exemplifying the "Who's on First" analogy, JC2WC, JCMA and JSC each interface separately with supported CINCs. No system currently exists to generate a single, integrated product.[1]

To be sure, some coordination occurs to the credit of participating organizations. For example, DARPA, DISA, and NSA formed a "virtual" Joint Technical Office to optimize the use of limited R&D funds and expedite delivery of info-protect technology, among other goals.[2] This union imaginatively capitalizes on three related but distinct focuses. DARPA concentrates on long-term, advanced R&D accomplished in concert with partners in industry and academia. DISA is DOD's first line of IO defense. It receives inputs from service CERTs to identify current problems, researches viruses, and attempts computer penetration to determine weaknesses. DISA is also parent to the automated systems security incident support team (ASSIST), a computer 911 service that helps defend against attacks and distributes warning notices concerning impending threats and computer vulnerabilities. Finally, NSA is the focal point for cryptography, telecommunications security, classified information systems security, and related R&D. While this cooperation promotes internal synergy, it does not characterize efforts throughout DOD.[3]

Notes

[1] Col Brian Fredericks, *Information Warfare: The Organizational Dimension*, Sun Tzu and Information Warfare, , NDU Press,1997, pg 88.

Notes

[2] *Memorandum of Agreement Between the Advanced Research Projects Agency, the Defense Information Systems Agency, and the National Security Agency Concerning the Information Systems Security Research Joint Technology Office*, March 1995.

[3] Col Brian Fredericks, *Information Warfare: The Organizational Dimension*, Sun Tzu and Information Warfare, NDU Press,1997, pg 88.

Chapter 8

"Cry 'Havoc and Let Slip The Dogs of War"

Who will lead the fierce IO charge? Who's point for investigating IO concepts and applications, strategizing R&D investment, sharing lessons learned, training and equipping for IO? Right now…no one, at any level. No organization in the US government has assumed responsibility for IO. The same shortfall exists at the Joint and service-levels. How should we organize for IO? Several proposals have surfaced, ranging from establishing an IW NAF; to forming an IW wing subordinate to each extant NAF; to creating a Global IO Center, subordinate to AF/XOI, and comprised of AIA's IO Center (IOC), AFIWC, the IW Battlelab and functional experts from ACC, AMC, AFSOC, and AFSPACE. One insightful article recognized the diversity of Joint efforts and recommend consolidation of Joint efforts under a flag officer.[1] National Defense Panel suggested giving the IO mission to SPACECOM with DISA transferred to SPACECOM a as a subordinate command. SPACECOM would manage the information infrastructure globally.[2] Yet another study recommended forming a DOD organization to attain Information Assurance, suggesting either USACOM or STRATCOM be given this responsibility.[3] Some consider a Unified Command approach to IO inappropriate arguing that IO is not a unique mission as is special operations and, therefore, does not need to be concentrated with a single CINC. Furthermore, IO is a problem endemic to

every CINC, whether functional or geographic in orientation. Each CINC must grapple with challenges inherent in IO. Actually, this logic supports the argument for charging one Unified Command with developing IO offensive and defensive capabilities. This consolidated approach enables other CINCs to focus on primary missions and precludes duplication of effort as each struggles to resolve similar problems. Another suggestion would be to detail IO as an additional duty to an "IO Officer," paralleling duties of the Air Force Safety Officer, and assigning an IO Officer at various organizational levels. This approach, however, would relegate IO to a support backwater and dilute DOD's ability to rapidly respond to attacks. Additionally, IO is a complex field, comprised of several distinct disciplines. A single "IO Officer" can not be adequately fluent in all.

Yet another suggestion was to transform parts of Air Intelligence Agency (AIA) into a Numbered Air Force (NAF), subordinate to Air Combat Command (ACC). This is actually how AF Special Operations Command evolved…first a NAF, then subsequently designated a Major Command (MAJCOM) with the establishment of USSOCOM. This approach, however, sorely misses the mark. A NAF lacks sufficient intensity and thrust, not to mention a four-star IO proponent, to effectively consolidate IO initiatives repeat throughout the Air Force and other services, as well. This approach also misses the mark with the IO NAF subordinated to an AF MAJCOM tasked with manning, equipping, and training, vice as an IO MAJCOM itself, subordinated to an operationally-focused IO Unified Command. The most serious shortcoming to the NAF proposal…it fails to capture the synergy extant in developing and testing IO concepts within the Joint realm. IO is complex…statement of fact. Due to its many and varied facets (PSYOPS, deception, EW, etc.), IO development and testing must not be restricted to a service

environment, only to be introduced into a Joint Task Force in a moment of crisis. A successful IO campaign depends on early and thorough joint integration. Solving this dilemma from an AF-exclusive perspective, i.e., the IO NAF, is not the answer. DOD needs an organizational solution at a much higher level to unite the plethora of ongoing IO efforts and to "Let loose the dogs of war", thus tackling the IO challenge head-on.

Centering the focus at the unified command level offers the best leverage of limited resources, as discussed below. The issue then becomes whether to organize geographically or functionally. At first glance, geographical organization seems most appropriate. Every combatant CINC needs to obtain Information Superiority. This approach allocates to each service the responsibility for IO training and equipping, and to each combatant CINC responsibility for IO planning and execution. A geographical orientation, however, places IO-related resource requirements in direct conflict with all other weapon systems and training requirements competing for finite command and service funds. It also allows each CINC to independently pursue avenues of info protect/info attack, fosters duplication of effort, and complicates the process of sharing lessons learned. The geographical approach echoes early calls to divide air forces, subordinating them to individual ground components.

Organizing IO functionally, creating a unified command for IO, will require Congressional legislation, as did the establishment of Special Operations Command. However, placing the responsibility for IO at the Unified Command level capitalizes on three long held military principles. The first, unity of command, "ensures the concentration of effort for every objective under one responsible commander…all efforts should be directed and coordinated toward a common objective…to gain most efficient

application."[4] This is especially critical today when organizations throughout DOD are recognizing vulnerability inherent in information infrastructures. Working groups and R&D efforts proliferate, due in large part to funds associated with IO efforts. Efforts are, to a large degree, uncoordinated among organizations and unevenly focused across the defensive and offensive facets of IO. Both time and funds are finite; they must be applied with concentrated intensity and coordinated among potential users. Vice Admiral Cebrowski, Navy's director of space and electronic warfare, agrees with this approach and likens it to nuclear warfare,

> We created an environment in which the various disciplines which contribute to nuclear warfare could come together and be managed as a mass rather than as a collection of career stovepipes. We need to do similar work with information technology.[5]

The second principle, that of mass, "focuses combat power at a decisive time and place....Mass is an effect that air and space forces achieve through efficiency of attack."[6] Functional organization under a single CINC allows focused identification of IO objectives for training, equipping, and R&D to develop tools for info protect and info attack. It would also generate synergy and expedite IO-related advances by sharing lessons learned among projects. The third principle, economy of force, "selects the best mix of combat power. To ensure overwhelming combat power is available, minimal combat power should be devoted to secondary objectives."[7] IO projects competing for funds can be systematically prioritized, weak points identified, and funds effectively allocated. This also capitalizes on resident IO expertise. Individuals well versed in IO tactics will be able to recommend the most effective mix of IO assets for applications in MOOTWs or crisis situations.

This new command might extrapolate elements of STRATCOM in planning and executing strategic IW operations. The destructive potential of strategic IW has often been compared to that of WMD; analysts equate resulting IW devastation to that of nuclear weapons. They argue that this similarity necessitates centralized planning, control, and execution. Indeed, Joint doctrine currently stipulates that IW execution must first be approved by the NCA. The analogy continues that this Unified Command, charged with centralized IO strategic planning, would have a counterpart to the Joint Strategic Target Planning Staff to develop the Single Integrated Information Warfare Operating Plan (SIIWOP) that could be expeditiously executed upon NCA direction. When asked if IO should be treated in the same manner as nuclear weapons, Vice Admiral Cebrowski agreed, "Yes, yes…we created an environment in which the various disciplines which contribute to nuclear warfare could come together and be managed as a mass rather than as a collection of career stovepipes. We need to do similar work with information technology."[8] Consider, however, the legacy of Strategic Air Command. The US invested significant resources to establish an organization that never launched a nuclear weapon, strategic or tactical. Should the US categorize IW in this same restrictive manner? Perhaps applying the standard rules of engagement and Law of Armed Conflict would negate the probability of US inflicting devastating, nuclear-type damage on an adversary nation's infrastructure? Strategists and targeteers should apply the following methodology when identifying IW targets…if the US would not employ conventional weapons against a specific target, e.g., bomb an adversary's stock market, then applying IW against that same target is probably inappropriate. The objective is to

devise a strategy that allows employment of a wide range of IO options, rather than an approach that precludes them.

Capitalizing on SOCOM's technique, the IO command would collocate IO teams with supported CINCs to assist the Joint Task Force as it plans and executes theater-level IO options. Thus, the command would offer an excellent balance of centralized control of strategic planning, budgeting, R&D, developing IO applications, and sharing lessons learned across the services, while facilitating combatant CINCs to incorporate these techniques into campaign plans and execute as needed. An IO command also offers the advantage of fully concentrating on IO challenges of the 21st century. From whence comes this command? DOD can not create Unified Commands out of thin air or even thinner DOD budgets. Cost effectiveness and expediency suggest leveraging momentum of existing organizations to form this proposed command.

One approach would be to use DISA as the nucleus for IOCOM. The DISA commander would be upgraded from a 3 to a 4-star position and serve as "CINC, IOCOM", representing DOD in national-level forums. IOCOM would consist of DISA, JC2WC, JCMA, JSC, and appropriate elements of JCS/J3/J6. IOCOM would collocate one team with each combatant CINC to interface with the theater IW cell. This team would integrate services currently provided by JC2WC, JCMA, and JSC. Service CERTs would continue to report possible IO-related discrepancies to DISA ASSIST. ASSIST would, in turn, serve as the DOD interface to the national-level IO crisis center recently established at the FBI. While elements of this concept have great merit, as discussed below, it has several flaws. Specifically, DISA is a large, cumbersome bureaucracy, not organized for expeditious support to warfighting CINCs. DISA is also a DC-based

organization, and as such, begs the question of providing critical warfighting support from within the beltway. And, most significantly, DISA does not possess Title 10 authority.

Assigning the IO mission to an existing command is a necessity, given constrained resources within the DOD and the overhead required to establish a new command. The question becomes, which CINC? SPACECOM is initially appealing considering the magnitude of battle-related information transmitted through space and the growing dependence on space-based assets. However, the two most crucial areas in the coming decade warranting concerted attention are IO and space. Assigning the IO mission to SPACECOM would, by definition, dilute the IO focus due to competing challenges and existing missions of that unified command. For this reason, SPACECOM is the most inappropriate extant command to be dual hatted as "CINC IO." Dual hatting space and information would detract from both missions at a crucial point in the evolution of each. At first glance, STRATCOM could vie as a potential candidate for "CINC IO", especially considering the ostensibly strong parallels in destructive potential between IW and nuclear attacks. However, STRATCOM's nuclear mission is critical, allowing no margin for error. Assigning IO here would either dilute attention from its primary nuclear mission or result in half-hearted development of IO concepts, applications, and offensive and defensive measures.

US Atlantic Command (USACOM) is, without a doubt, the best repository for the critical IO mission for two significant reasons. First, USACOM is currently charged with joint training and physical defense of CONUS. This mission responsibility could be logically expanded to include defense of DOD's military automated infrastructure. In

this capacity, USACOM would also be the designated DOD representative at the national-level in coordinating the defense of the civilian infrastructure, critical to successful execution of military operations. Second, the mission and focus of USACOM is currently evolving. The Defense Reform Initiative recently announced by the Secretary of Defense will realign the following five Joint activities to USACOM effective 1 October, 1998: Joint Warfighting Center (JWFC), Joint Communications Support Element (JCSE), Joint Command and Control Warfare Center (JC2WC), Joint Battle Center (JBC), and the Joint Warfighting Analysis Center (JWAC). Other joint organizations are being considered, as well. The synergy is real, it's happening, and the operational potential is...well...exciting!

This realignment will streamline the Joint Staff by divesting operational functions and organizations to ACOM, thus enabling the Joint Staff to better concentrate on its primary role of formulating policy and guidance. The realignment will also strengthen USACOM's role in joint functional training and improve joint force integration, particularly in the evolution of advanced joint tactics, techniques, procedures, and equipment. Incorporating these organizations into USACOM yields the opportunity to regularly develop, test, evaluate, and integrate IO techniques within the joint arena. Once integrated, USACOM holds the potential for establishing a sorely needed Joint Task Force for IO, responsive to combatant CINCs.[9] No longer would an Information Protect crisis team be formed out of necessity at the Joint Staff. In sum, USACOM could propel the DOD towards both resolving defensive vulnerabilities and developing offensive skills, all the while providing the perfect opportunity to "Train in peace as you would fight in war." The end result will be vastly improved services to warfighting CINC's.

Given this organizational transition and a lack of a concentrated, singular mission focus as extant in both STRATCOM and SPACECOM, USACOM is poised to assume the role of "CINC IO"…if DOD leadership and leaders of USACOM in particular, recognize the timing and seize the opportunity.[10]

Notes

[1] Col Brian Fredericks, *Information Warfare: The Organizational Dimension*, Sun Tzu and Information Warfare, NDU Press,1997, pg 96.

[2] *Transforming Defense:National Security in the 21st Century*, Report by the National Defense Panel, December 1997, pg 72.

[3] Kevin J Kennedy, et al, *Grand Strategy for Information Age National Security*, Air University Press, Maxwell Air Force Base, Al, August 1997, pg 54.

[4] Air Force Doctrine Document (AFDD) 1-1, *Air Force Basic Doctrine*, September 1997, pg 12.

[5] Jason Sherman, *Infowar? What Kind of a Defense?,* Armed Forces Journal, August 1997.

[6] Air Force Doctrine Document (AFDD) 1-1, September 1997, pg 16.

[7] Ibid., pg 18.

[8] Jason Sherman, *Infowar? What Kind of a Defense?,* Armed Forces Journal, August 1997.

[9] Ibid.

[10] Briefing, *CCA Transition Update to CINCUSACOM*, January 28, 1998.

Chapter 9

Conclusions

This was a lengthy but important journey, spanning thousands of years from Sun Tzu to the Information Age. That information has always been a valuable commodity is unquestioned. What has changed is the amount, speed, and methods by which information is transmitted and received. Technologically advanced, democratic societies are most dependent, and therefore most vulnerable to the interruption, corruption, or manipulation of that data flow. A host of potential antagonists noted this weakness, several of whom already skillfully wage and win information wars against the US. We can expect these attacks to increase in number and severity due to our susceptibility, and the ease and low-risk associated with such attacks.

While some analysts do not credit a strategic "electronic Pearl Harbor" in the next decade, they strongly predict the probability of multiple and widespread tactical Information Warfare attacks within this same time frame. Others believe this projection is severely underestimated based on the February 1998 cyber attacks on DOD. Despite the difference in timeframe, the message is constant--we should take immediate steps to shore up our defenses. Consider now the, some say 'inevitable,' arrival of the ultimate strategic IW attack…granted, a decade hence. How long does it take the DOD acquisition community to ramp up and deploy a major weapon system? Ten

years…more? Suggestion is that the US is already behind the power curve in preparing our defenses against this looming threat. However, we must keep the challenge in perspective. Even if the DOD focused enormous effort into resolving this dilemma, this could alleviate only a small part of America's vulnerability, as the DOD relies significantly on the civilian infrastructure. Private and public entities must also act in earnest. But, that aspect must be left to another paper. Consequences of inaction, to include step-by-step political, economic, and social unraveling of the US, are depressingly and vividly depicted in articles such as "The Great Cyber War of 2002", "How We Lost the High-Tech War of 2007: A Warning from the Future", and "All Under the Sun." As a country, we don't want to go there but may not have a choice if adversaries are calling the shots.

The DOD continues to base US defense posture for the 21st century on assumptions of Information Dominance and Dominant Battlespace Awareness. It does so despite the large number of publicized attacks on military and civilian infrastructures; interdependency of the GII, NII, and DII; and vulnerability to all aspects of IW recognized at the highest levels of the US government. What must we do to make our defense policy truly viable? Falling back on nuclear strategy, we must establish a credible IO deterrence. Key to this capability is attaining a credible IO defense, convincing adversaries that our principle systems are secure, i.e., Information Assurance. No one today would argue that air superiority is critical to winning the ground war. In a similar vein, Information Superiority can not be attained without Information Assurance. We must also convince adversaries that the US also possess and is willing to employ a

credible IO offensive arsenal. DOD must also develop skilled staff personnel fluent in devising and executing plans applying all aspects of IO.

Has DOD stepped up to the plate? Somewhat. Secretary of Defense Chaney announced the bold proposal to establish the IO position within ASD/C3I. The Joint Staff is realigning staff vs. operational missions. USACOM is poised and full of potential to make headway on these pressing IO issues. Agencies throughout the AF and other services are scrambling for IO-related projects. The good news…we are shoring up our defenses, slowly. The bad news: many senior leaders doubt the efficacy of IO and demonstrate great difficulty breaking the paradigm of industrial-level war. These individuals impede the transition of funds from the kinetic force to prepare for wars of the 21st century. Furthermore, the DOD is still caught in a bureaucratic quagmire of IO terminology, impeding substantive headway due to a war of words. We must get beyond this. While we dissect written nuances via staff summary sheets, countries such as Russia, Cuba, China, and others are actively developing IW tools…to say nothing of the non-nation state adversaries.

What is the proposed solution? How can we get there? Five years hence, what should be the line up of extant Unified Commands? "Be bold in your recommendations!" "Step out on that limb!"…such advise adds spice to intellectual think pieces. Here is that recommendation, boldly sitting on the limb! Looking five years hence, USACOM will be the undisputed center of gravity for IO. The name will be amended to reflecting its primary mission, defense of the US homeland…perhaps the "America Command" (AMCOM). In this respect, AMCOM would have a geographic focus much like EUCOM for European region and PACOM for the Pacific region. Second, in addition to

elements divested from the Joint Staff, other elements should also be resubordinated to this command, specifically: JCMA, JSC, appropriate elements of JCS/J3/J6, and IO elements within DISA. Following the SOCOM model, AMCOM would collocate one team with each combatant CINC to interface with the theater IW cell. This team would integrate services currently provided by JC2WC, JCMA, and JSC. JC2WC teams already interface closely with combatant CINC's. It provides a ready-made nucleus for an IO Joint Task Force (JTF) which would work for CINC AMCOM but would deploy to and be operationally controlled by supported CINC, upon direction by the National Command Authorities.

Another element of AMCOM, the Joint Information Warfare Center (JIWC), would alleviate a significant shortfall recognized by national-level studies. JIWC would provide a centralized joint organization to monitor the health of the DOD automated infrastructure, warn of impending attack, respond effectively to minimize and assess damage, and initiate efforts to reconstitute. Located at Kelly AFB, the JIWC would capitalize on expertise of the collocated JC2WC, HQ AIA, AFIWC, AFCERT, and IW Battlelab. JIWC would include liaison officers from service components IO agencies (e.g., Air Force AFIWC, Army LIWA and Navy NIWA) and representatives of national-level agencies, such as the FBI and NSA's Information Operations Technical Center (IOTC). Service CERTs would report possible IO-related discrepancies to a Joint ASSIST agency which would also interface with the JIWC.

The Air Force must restructure to centralize and streamline IO operations. HQ AIA would become the Air Force's IO MAJCOM, serving as the Air Force component to the IO Unified Command. This migration would necessitate AIA severing its organizational

ties to the Air Staff, as currently exist in AIA's status as a FOA. This change parallels the ongoing restructure of the Joint Staff and would likewise allow AF/XO to concentrate on policy and guidance issues, vice IO operational support to combatant CINCs. AIA, as an IO MAJCOM, must sharpen its IO focus by divesting functions supporting Air Staff. This can be accomplished by transforming the DC-based 497 IG into a separate Forward Operating Agency (FOA) reporting to HQ AF/XO, and augmenting with necessary manpower. 609 IS should be disbanded because of capabilities resident in AIA or resubordinated from ACC to AFIWC. This would eliminate redundancy and detrimental competition with other Air Force IO elements. AFCC and Air Force Weather Agency, two other significant IO-related organizations, should be incorporated into this AF IO MAJCOM. AIA's relationship to AMCOM would then parallel AFSOC, with heavy emphasis on supporting combatant CINCs.

AMCOM should be allocated its own Program Element (PE), paralleling SOCOM's MPF 11. This would alleviate a major criticism uniformly specified by PCCIP, DSB, and NDP regarding insufficient, sporadic, and uncoordinated IO expenditures. Establishing an IOCOM PE would also resolve the impediment of convincing the conventionally focused, military establishment to shift kinetic funds to IO initiatives, a problem experienced by Special Forces. Vice Admiral Cebrowski succinctly stated that preparing an adequate IW defense will require "a fundamental reallocation of resources."[1] AMCOM could seriously concentrate R&D funds to eliminate current and very fundamental shortfalls such as real-time detection, identification, and response to an information attack. Additional R&D effort must be focused to rapidly identify damage and reconstitute. While DOD is capitalizing on commercial R&D, unexplored but

militarily relevant areas exist which are either too speculative or not applicable for commercial investment. AMCOM could spur investment in these areas. Other benefits resulting from centralized budget management and execution: methodical dissemination of lessons learned, coordinating contracts to maximize resource investment; oversight to ensure security is prerequisite in future system design, and focused attention on training and retention of IO specialists. AMCOM would also comprise a single and effective interface with government and commercial organizations working towards the common goal of Information Assurance.

In short, if DOD sustains bureaucratic inertia despite the plethora of IW attacks and insightful predictions of IW attacks to come…if DOD fails to seize the momentum offered by establishing AMCOM, then shame on us. On the other hand, DOD could astutely give AMCOM the IO lead. AMCOM would unabashedly forge scarce resources and joint expertise into a concentrated pursuit of Information Assurance and offensive IW applications. The result…credible IO deterrence. This will enable senior DOD leaders to build their castles, our national security policy, on a foundation much firmer than sand. This proposed solution is definitely attainable. It seems fitting to close with another insightful observation from Douhet…

> Victory smiles upon those who anticipate the changes in the character of war, not upon those who wait to adapt themselves after the changes occur…Those nations who are caught unprepared for the coming war will find, when war breaks our, not only that it is too late for them to get ready for it, but that they cannot even get the drift of it. [1]

Notes

[1] Douhet, *The New Form of War*, Air War College Strategy, Doctrine, and Airpower, Book II, Air University, 1998, pg 28.

Bibliography

Arquilla, John, *The Great Cyberwar of 2002*, Wired Magazine, February 1998

Brennan, Rick and R. Evan Ellis. *A Case Study of Somalia,* April 18, 1996 SAIC Project Number: 03-9847-000 SAIC Document Number: 96-6960 & SAC Prepared for the Office of the Secretary of Defense, Net Assessment

Brewin, Robert and Heather Harreld, *DOD Adds Attack Capability to Infowar/Move Follows Latest Round of Hacks,* Federal Computer Week, March 2, 1998

Bryan, Kenneth D. *Shop Talk: PACOM Team,* Cyber Sword, Vol. 1, Number 2, Fall 1997

Cajigas, Anthony. The Secret Battlefield, Computer Warfare Contingencies II, http:/www.infowar.com/mil_c4i/cajigas/mil_c4ize.html-ssi

Campen, Alan D. It's Vulnerability, Not Threat—Stupid. Information Assurance Needs Patching More Holes, Less Chasing Foes. infowar.com

Correll, John T. *War in Cyberspace*, Air Force Magazine, January 1998

Dornheim, Michael A. *Bombs Still Beat Bytes*. Aviation Week and Space Technology, January 19, 1998

Dunlap, Charles J. Jr. 21st Century Land Warfare: Four Dangerous Myths, Parameters, Autumn 1997

Dunlap, Charles J. Jr. How We Lost the High-Tech War of 2007: A Warning from the Future, The Weekly Standard, 29 January 1996

Fredericks, Brian. *Information Warfare: The Organizational Dimension*, Sun Tzu and Information Warfare, NDU Press, 1997

Futrell, Robert Frank, *AWPD-1: Air Planning for War*, Strategy, Doctrine, and Air Power Book II, AWC, AU Press, 1998

Goral, Col Frank I., USMC and William R. Swart. *Information Superiority: Enabler of the Future.* Cyber Sword, Vol. 1, Number 2, Fall 1997

Gordon, Michael R. and Trainor, Bernard E. *Instant Thunder*, Strategy, Doctrine, and Air Power Book II, AWC, AU Press, 1998

Huber, Arthur, et al. Virtual Combat Air Staff: The Promise of Information Technologies, RAND, 1996

Johnson, L. Scott, Toward a Functional Model of Information Warfare, infowar.com, October 1997

Kennedy, Kevin J. et al. *Grand Strategy for Information Age National Security*, Air University Press, Maxwell Air Force Base, Al, August 1997

Millett, Allan R., *Patterns of Military Innovation in the Interwar Period,* Strategy, Doctrine, and Air Power Book II, AWC, AU Press, 1998

Mitchell, Brig Gen William, *The Development of Air Power*, Strategy, Doctrine, and Air Power Book II, AWC, AU Press, 1998

Peters, Whit and Richard Marshall. Briefing *Defensive Information Operations*, USAF Information Operations Conference, October 18, 1997

Schafer, Suzanne M. *Hackers Invade Pentagon Computers*, Associated Press, February 26, 1998

Sherman, Jason. *Infowar? What Kind of a Defense?,* Armed Forces Journal, August 1997

Stein, Dr. George J. Jane's Special Report: US Information Warfare, Jane's Information Group, Alexandria, Va. 1996

Stoll, Clifford. The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage, NY: Doubleday; 1989

Szafranski, Richard, *An Information SIIOP*, infowar.com

Toffler, Alvin. *War and Anti War*, Warner Books Inc, NY, 1993

Xuaheng, Wang, et al. China: Information Revolution, Defense Security, Beijing Jisuanji Shijie (China Computerworld), August 11,1997

Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2nd Edition, July 1996, by Joint Staff

Executive Order 13010, *Critical Infrastructure Protection,* July 1996

Remarks by Stevan Mitchell, Commissioner PCCIP, at DOD Worldwide Antiterrorism Conference, August 21, 1997

Remarks by Stevan Mitchell, Commissioner PCCIP, at DOD Worldwide Antiterrorism Conference, August 21, 1997

Remarks by Stevan Mitchell, Commissioner PCCIP, at Howard University's JFK School of Government, September 20, 1997

Briefing, Information and Communications Sector: The Nation's Central Nervous System, Nancy J Wong, PCCIP Commissioner

Briefing, CCA Transition Update to CINCUSACOM, January 28, 1998

Power of the Image, History Channel broadcast

Pentagon Looks for Answers to Massive Computer Attack, Defense Information and Electronics Report, February 13, 1998

Attack Software Plays Key Offensive Role, Aviation Week and Space Technology, January 19, 1998

Active Measures Key to Soviet Discrediting Campaign, Washington Times, May 23, 1985

Global Engagement: A Vision for the 21st Century Air Force

Joint Vision 2010

Military, Industry Partners Grab Information Systems' Brass Ring, Signals Magazine September 1997

Air Force Doctrine Document (AFDD) 1-1, *Air Force Basic Doctrine*, September 1997

Transforming Defense: National Security in the 21st Century, Report by the National Defense Panel, December 1997

Military, Industry Partners Grab Information Systems' Brass Ring, Signals Magazine, September 1997

Memorandum of Agreement Between the Advanced Research Projects Agency, the Defense Information Systems Agency, and the National Security Agency Concerning the Information Systems Security Research Joint Technology Office, March 1995

Cyber Terrorism, Secure Computing, July 1997

DISTRIBUTION A:

Approved for public release; distribution is unlimited.

Air War College
Maxwell AFB, Al 36112